空気圧コントロールシステムにおけるインタロックシステムに関する研究

２０１３年度　理工学研究科

博士学位請求論文（要旨）

空気圧コントロールシステムにおけるインタロックシステムに関する研究

学位請求者　新領域創造専攻
中村　瑞穂

内　容　の　要　旨

１．本研究の問題意識と目的

空気圧システムは，故障や制御の誤りによって，高圧空気の噴出や破裂による部品の飛来など，人に危害を生ずる可能性がある．本論文では，空気圧システムの圧力調整に伴う危険側誤りに関する調査と，それに伴うリスクを解消するインタロックの実現可能性について論理的な検討を行う．その結果，窓特性を有する監視によって空気圧システムがフェールセーフを可能とするインタロックシステムとして実現し得ることを示す．さらに，国際規格による安全の見方から考察を行い, ISO13849 で示される安全関連系との相違点の明らかにして，実用的なインタロックシステムの空気圧システムへの適用について考察する．

なお, 現状において安全の妥当性は国際規格 ISO12100 の体系に準拠する方法と，安全(確認)の原理に基づいて論理的に行う方法とに二分されている．本報告は，両者の違いを明らかにして，相互に整合しあうことを示すことも目的に含まれる．

2.　本研究の構成ならびに各章の要約

空気圧システムは，工作機械，輸送機械，化学工業，造船，車両，自動車など製造業を中心に幅広く利用されている．さらに，その利用は工場の自動化ラインのように人間と離れて使用される機器から医療機器などの人間と密接な状態で使用される機器まで広範囲に及び，機器によって利用環境が大きく異なる．

空気圧システムの設計にあたって，ISO12100-1 では「機械がく類の設計時に考慮すべき危険源」について同定し，保護方策を行うことが規定されている．しかし，空気圧システムは多種多様に利用されており，利用する機器によっては，人間が持ち運びできる簡易な機器も含まれ，ユーザーの都合により簡単に使用環境を変えることが可能な機器も多く存在する．

しかし，空気圧は，誤った使用がなされれば重大な被害をもたらす危険源であり，安全の使用条件（例えば最大許容圧力）は設計段階で明確に示され，それに準拠した使用が本来なされなければならない．しかし，ユーザーの都合により機器の使用条件が変更され，そのために破裂等による事故（危害）が生じている．本研究では，安全の条件に準拠した使用がなされるよう監視するためのインタロックシステムについて論理的検討を行う．

本論文では第 1 章で研究の背景，目的，構成，用語の定義と表現について説明している．

第 2 章では空気圧システムの基本構造とそれに関係する国際規格，および安全システムを構成するために基本となる安全（確認）の原理を取り上げて，本研究の立場を明確にする．国際規格はリスクベースの安全を基調とし，そのため強度信頼性の見方から，空気圧システムの安全性はコンポーネントの故障の発生確率を小さくすることで確保されるとしている．同様に，制御も危険側誤りの発生確率を小さく抑えるよう求めており，現実に残る危険側故障による危害（事故）に対する対応を求めていない．例えば，国際規格では動力遮断の必要を認めるが，安全システムの条件として具体的構造を規定していない．特に，レギュレータの圧力上昇側の故障は重大な

危険側故障であるが，動力遮断が曖昧であるため“妥当”とされる安全が確保されているとは言えない．このように，国際規格では，安全機能を「リスク低減のための機能」と解し，その構造を明確にしていないため，本研究では，まず，安全（確認）の原理に準拠して安全のあるべき構造について論理的検討を行い，改めて，国際規格の安全の観点から評価を行う手順に従うものとにする．特に，第 2 章では残留リスクの影響を遮断する動力遮断についての論理的検討を行っている．

第 3 章は空気圧システムの構成例を用いて，システム構成する各種空気圧コンポーネント（13 種類）について FMEA（Failure Mode and Effects Analysis）を適用して故障モードの検討を行っている. FMEA による分析の結果，220 件の故障モードを抽出した．その中でシステム内部の圧力上昇側の故障モード（危険側故障）が 15 件，システム内部の圧力低下側の故障モードが 140 件，安全に影響しない故障モードが 65 件である．なお，FMEA が適正であることは，BIA-Report6/97e，ISO13849-2 と比較することによって，確認している．

また，空気圧コンポーネント（13 種類）の危険側故障は P1（動力調整部圧力），P0（駆動系圧力）の圧力の上昇として現れるが，低下側の誤りも危険側となる可能性を指摘し，そのため，空気圧システムの危険側故障は，圧力の上昇と低下の両方を監視すべきとする結論を得た．

現状の空気圧システムではコンポーネントの危険側故障が存在するばかりでなく，圧力の低下側にも危険側故障である可能性があり，圧力の上昇・低下の監視とレギュレータの危険側故障について動力遮断を実行するインタロックが必要であることを示す．特に，レギュレータやリリーフ弁等の故障が危険な圧力上昇となる重大な危険側故障となるため，インタロックシステムにおける動力遮断の重要性を明らかにしている．

第 4 章では，FMEA による危険側故障に関する分析結果に基づき，そのリスク発生を本質的に解消する動力遮断機能を持つインタロックの実現可能性について論理的な検討を行っている．検討の結果，窓特性を有する監視によってフェールセーフ・インタロックが実現し得ることを示す．そのためには，基本的には，空気圧システムにおける圧力制御がフェールセーフの条件（安全（確認）の原理に基づくユネイトな論理的関係）を満たすか否かを明らかにする必要がある．そこで，空気圧システムの動力調整部 P1 に注目し，駆動系との分離点に圧力の上昇と低下を検出する窓による監視（以降，“窓監視”とする）を導入し，危険側誤りの発生を動力遮断によって回避するインタロックが実現可能であることを示した．さらに，第 4 章では，フェールセーフな窓監視に用いるウインドゥ・コンパレータと危険側誤りを監視するセンサについて，その機能と安全上必要とする構造について説明している．このような窓監視を用いることによってインタロックがフェールセーフに適う条件で実現可能であることを，安全（確認）の原理に基づく論理的ユネイト性を用いて証明している．すなわち，危険側故障を認めながらも，動力遮断と連動することで，その影響を解消するとする新しいフェールセーフ構成法であることを明らかにした．これらの検討により，インタロックシステムは危険側誤りの監視および動力遮断構造を持ち，危険側故障の影響（危害）を抑制するフェールセーフ・インタロックシステムであることを結論としている．

第 5 章では国際規格で規定される安全関連系とインタロックシステムとの整合性についての検討を行っている．

本研究で対象とするインタロックシステムが基礎とする安全コンセプトを明確にし，その妥当性について明らかにする．次いで，機械安全に関する国際規格 IS12100 及び ISO13849-1 による安全の基本原理を明確にして, 安全制御の見方から，安全コンセプトと国際規格の安全の比較検討を行い，このインタロックシステムの国際規格との整合性について検討している．また，インタロックシステムについて, 改めて ISO13849-1 で規定される安全関連系としての評価を行い，インタロックシステムは，遮断弁を用いて故障時，空気圧システムから切り離す構成であるため，空気圧コンポーネントの危険側故障はすべて，インタロックシステムの遮断構造に集約され，遮断弁の特性でシステム全体のフェールセーフが実現されることを明らかにしている．

第 6 章では現状の，異なる 2 つの安全の妥当性確認手法である安全（確認）の原理と国際規格の比較を行い両者が基本的に同じとみなし得ると考察している. さらに，インタロックシステムの構成において安全（確認）の原理における構成法が国際規格に基づく構成法よりも優れた安全関連系の構成が可能であると結論付けている．

今後の課題としては EN764-7（火なし圧力容器の安全システム）で規定されている制御による安全の理論構築を目指し本研究で提案しているインタロックシステムの窓監視，動力遮断構造を安全システムとしてレギュレータによる調整制御に関する理論（安全制御の原理）の提案と検討を行う予定である．